Jurnal Ilmiah Setrum

Volume 9 , No. 1, Juni 2020 **p-ISSN : 2301-4652 / e-ISSN : 2503-068X**

Peningkatan Kinerja Sistem Keamanan Pada Proses pensinyalan Dalam Vertical Handover MIPv6

Supriyanto[1], Daniel Barita[1]

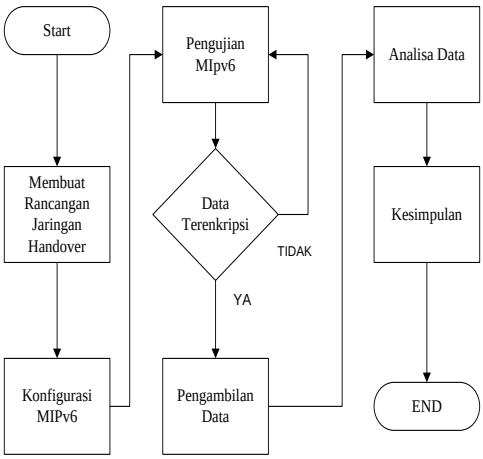
[1]Jurusan Teknik Elektro, Fakultas Teknik, Universitas Sultan Ageng Tirtayasa, Banten.

Informasi Artikel

Naskah Diterima : 3 Maret 2020
Direvisi : 15 April 2020
Disetujui : 15 Mei 2020

***Korespodensi Penulis :**
supriyanto@untirta.ac.id

Graphical abstract



Abstract

The development of mobile technology is increasing every year as well as users of mobile devices. Vertical Handover (VHO) is one of the technological developments that helps mobile users and communicate or share data easily with each other. VHO requires an IPv6 address on a mobile device called the mobile internet protocol (MIPv6). However, MIPv6 has a gap that makes it vulnerable to attack when carrying out a handover process, especially during the Binding Update process. One way to secure MIPv6 is to use the IPsec tunnel method with ESP header. The encryption that will be used in this study is 3DES and AES. Based on the research carried out AES encryption is superior to 3DES with throughoput values of 25.25 Mbit / s and 21,978 Mbit / s, respectively. With time generating 0.019 ms AES packet while 3DES requires 0.121 ms.

Keywords: Vertical Handover, MIpv6, AES, 3DES.

Abstrak

Perkembangan teknologi mobile semakin meningkat setiap tahunnya begitu juga dengan pengguna perangkat mobile. Vertical Handover (VHO) merupakan salah satu perkembangan teknologi yang membantu para pengguna mobile dan berkomunikasi ataupun berbagi data dengan mudah satu-sama lain. VHO membutuhkan alamat IPv6 pada perangkat mobile yang disebut dengan mobile internet protocol (MIPv6). Namun, MIPv6 memliki celah yang membuatnya rentan diserang ketika melakukan proses handover terutama pada saat proses Binding Update. Salah satu cara mengamankan MIPv6 adalah dengan menggunakan IPsec metode tunnel dengan ESP header. Enkripsi yang akan digunakan pada penelitian kali ini adalah 3DES dan AES. Berdasarkan penelitan yang dilakukan enkripsi AES lebih unggul dibandingkan 3DES dengan nilai throughoput masing-masing 25,25 Mbit/s dan 21,978 Mbit/s. Dengan waktu generate packet AES 0,019 ms sedangkan 3DES memerlukan waktu 0,121 ms.

Kata kunci: Vertical Handover, MIpv6, AES, 3DES

1. PENDAHULUAN

Perkembangan teknologi *mobile* semakin meningkat setiap tahunnya, hal ini ditunjukkan dengan semakin banyaknya pengguna teknologi *mobile* yang menyebabkan semakin tingginya permintaan akses layanan komunikasi. Permintaan akses layanan komunikasi yang semakin banyak harus diimbangi dengan pelayanan terbaik dengan memperhatikan QOS (Quality of Service), area jangkuan, biaya, dan sebagainya.

Salah satu perkembangan teknologi yang mendukung pengguna mobile adalah Vertical Handover (VHO). VHOO merupakan perubahan tipe konektivitas dari titik jaringan yang digunakan untuk mengakses infrastuktur pendukungnya, biasanya untuk mendukung pergerakan. Algoritma VHO adalah proses yang dilakukan oleh perangkat untuk membuat keputusan VHO dan memilih jaringan target dari jaringan kandidat [1]. Untuk mendukung VHO dibutuhkan sebuah alamat *Internet Protocol* versi 6 (IPv6) yang memiliki jumlah alamat yang jauh lebih besar dari versi 4 yaitu sebesar sekitar 3,4 x 10^{38}, perangkat *mobile* yang mendukung IPv6 disebut *mobile IPv6*(MIPv6).

Mobile IPv6 adalah teknologi jaringan komputer yang mendukung mobilitas *user* untuk berpindah dari satu jaringan ke jaringan lain tanpa harus berganti alamat IP [2]. Teknologi *mobile* juga merupakan sebuah teknologi yang memiliki perkembangan yang cepat, karena sifatnya yang mudah dibawa dan praktis. Teknologi *Wireless* pada teknologi *mobile* sudah sampai pada generasi keempat atau 4G. Jaringan nirkabel 4G terdiri dari jaringan akses kabel dan nirkabel yang berbeda [3].

Mobile IPv6 rentan terhadap serangan saat terjadinya proses *Binding update*. Ketika proses handover *mobile node* harus diproteksi IPsec dengan meotde *tunnel* menggunakan *Encapsulating Security Payload* (ESP) [4]. Terdapat beberapa metode enkripsi yang dapat digunakan pada MIPv6 yaitu Triple Data Encryption Standard (3DES) dan Advanced Encryption Standard.3DES adalah jenis kriptografi terkomputerisasi di mana algoritma cipher blok diterapkan tiga kali untuk setiap blok data. AES merupakan *block chipper* simetris yang menggunakan 128 bit block,

Beberapa penelitian telah dilakukan untuk melakukan pengujian terhadap kemampuan 3DES dan AES. Pada penelitian yang dilakukan Noura Aleisa [5] dapat diketahui bahwa 3DES memiliki ketahanan terhadap serangan *brute force, interpolation cryptnalysis* dan kurang cocok untuk mengenkripsi data dengan ukuran besar sedangkan AES memiliki ketahanan yang lebih kuat daripada 3DES dan dapat digunakan pada perangkat *mobile* karena lebih ringan.

Sedangkan pada penelitian [6] dapat diketahui bahwa AES memiliki keunggulan pada aspek keamanan dan kecepatan dalam pembuatan paket lebih cepat dari 3DES. Kedua penelitian yang telah disebutkan tidak menjelaskan tentang performasi dari 3DES dan AES pada jaringan MIPv6, sehingga pada penelitian kali ini akan diteliti tentang performasi 3DES dan AES pada jaringan MIPv6.

2. TINJAUAN PUSTAKA

Jaringan komputer adalah sistem terdistribusi yang terdiri dari dua atau lebih komputer/perangkat untuk berkomunikasi dan berbagi informasi antara satu dengan yang lainnya. Salah satu jaringan komputer yang dapat mendukung komunikasi yang lancar dan handal adalah *handover*.

2.1.1 Handover

Handover merupakan proses perpindahan *mobile node* (MN) dari *home agent* (HA) ke *foreign agent* (FA). Ketika MN melakukan perpindahan jaringan dari HA ke FA maka MN akan mendapatkan alamat baru, lalu MN akan memberikan pesan *Binding Update* (BU) kepada HA untuk memberitahukan alamat barunya sehingga pengguna lain yang terhubung dengan HA dapat berkomunikasi dengan MN menggunakan alamat MN ketika berada di HA. Setelah HA mendapatkan alamat baru dari MN maka HA akan mengirimkan pesan *Binding Acknowledgment* yang memberitahukan MN bahwa alamat barunya telah disimpan.

2.1.2. Mobile Internet Protocol version 6 (MIPv6)

MIPv6 merupakan sebuah standar mobilitas pada jaringan IPv6. MIPv6 memungkinkan sebuah perangkat untuk melakukan proses handover. IPv6 digunakan karena memiliki jumlah alamat yang lebih banyak dibandingkan dengan IPv4 yaitu sebanyak 3,4 x 10^{38} alamat.

2.1.3. Penelitian Terkait

Pada penelitian yang dilakukan oleh Suwega Dreswanto[7] dapat diketahui performansi dari MIPv6 pada *vertical handover*. Peneliti menjelaskan bahwa MIPv6 diperlukan untuk *vertical handover* dan peneliti mengetahui bahwa performasi MIPv6 pada *vertical handover* lebih rendah daripada *horizontal handover* peneliti menggunakan aplikasi ftp untuk menganalisi performa jaringan yang ada, pada penelitian tersebut peneliti juga menyatakan bahwa handover akan mempermudah pengguna untuk berbagi data walaupun berapa pada *access point* yang berebeda.

Pada penelitian yang dilakukan Charles[4] dapat diketahui bahwa MIPv6 memiliki celah keamanaan terutama pada saat proses *Binding Update*, diaman penulis menyerankan menggunakan IPsec header untuk melindungi MN. Pada penelitian yang dilakukan Hamdan.O.Alanazi[6] dapat diketahui bahwa diantara 2 jenis enkripsi 3DES dan AES, AES memiliki keunggulan dari berbagai factor dibandingkan dengan 3DES yang dibuktikan dengan cara mencari kemungkinan kunci enkripsi aes dan 3des diketahui oleh pihak lain.

3. METODE PENELITIAN

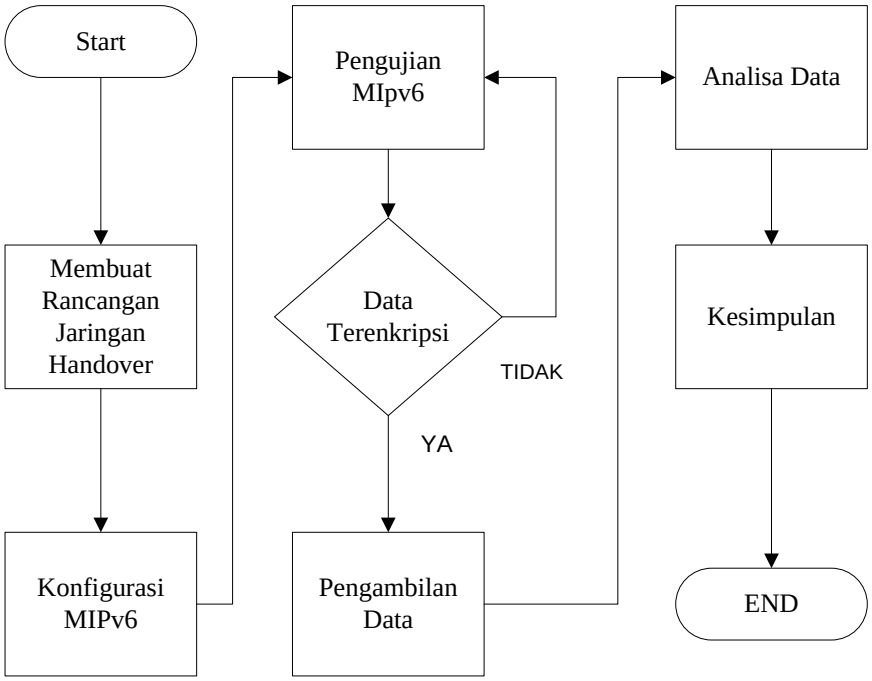
3.1. Metode Penelitian

Penelitian dilakukan dengan melakukan beberapa tahapan yaitu:

a. Studi literatur mengenai penelitian sebelumnya untuk menentukan permasalahan yang akan diteliti
b. Merancang jaringan yang digunakan selama penelitian yang dibagi menjadi perancangan hardware berupa raspberry pi 3 b+ dan laptop dan perancangan software berupa UMIP.
c. Melakukan pengujian handover pada jaringan MIPv6 yang sudah dibuat.
d. Melakukan beberapa pengujian handover dengan data paket yang telah dienkripsi menggunakan 3DES dan AES.
e. Pengambilan data pada jarigan yang telah dibuat.
f. Melakukan Analisa terhadap data yang telah dikumpulkan.
g. Penarikan kesimpulan.

3.2. Diagram Alir Penelitian

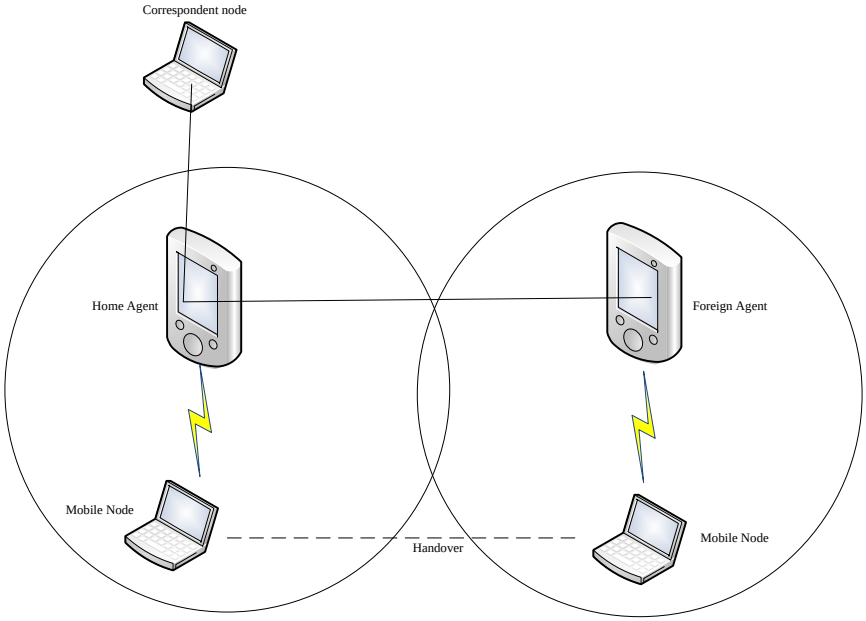
Proses perancangan penelitian dapat digambarkan melalui diagram alir pada Gambar 1.



Gambar 1. Diagram Alir Penelitian

3.3. Perancangan Penelitian

Penelitian ini dilakukan dengan pertama-tama mempersiapkan peralatan *home agent(*HA), *foreign agent*(FA), *correspondent node*(CN), dan *Mobile node*(MN). Perangkat sudah tersedia akan dilakukan instalasi perangkat lunak yang digunakan guna mendukung fitur MIPv6 dan pemberian alamat IPv6 pada setiap *node* sehingga dapat berkomunikasi dalam jaringan. Setelah setiap keperluan sudah dilakukan, dilakukan pengujian dengan cara MN melakukan ping kepada CN ketika sudah melakukan handover dari HA ke FA Berikutnya dilakukan pengujian throghtput menggunakan iperf proses pengujian dilakukan pada enkripsi 3DES dan AES.



Gambar 2. Topologi Vertical Handover MIPv6

4. HASIL DAN PEMBAHASAN

4.1. Hasil Pengujian Data

Hasil pengujian implementasi 3DES dan AES pada MIPv6 dilakukan untuk mendapatkan data performansi tiap enkripsi. Ketika melakukan handover MN dari HA ke FA, MN mendapatkan alamat IPv6 baru dari FA, tetapi CN tetap dapat berkomunikasi dengan MN menggunakan alamat IPv6 MN saat berada di HA, hal ini dapat terlihat ketika melakukan pengujian delay dan jitter seperti terlihat pada Tabel 1. Selanjutnya dilakukan pengujian throughtput dan overhead dari MN ketika data yg dikirim sudah dienkripsi menggunakan 3DES dan AES dan dapat diketahui juga berapa lama waktu paket hasil enkripsi dibuat sebelum dikirimkan dari MN ke CN.

4.1.1 Hasil Pengujian Delay dan jitter MN ke CN

Pada pengujian kali ini dilakukan untuk mengukur hasil delay dan jitter dari MN ke CN yang sudah dienkripsi.

Tabel 1. Nilai Rata-Rata Pengujian Delay dan Jitter

Enkripsi	Delay	Jitter
3DES	27.48 ms	39.56 ms
AES	34.68 ms	52.73 ms

Seperti terlihat pada Tabel 1. Hasil 3DES memiliki delay dan jitter yang lebih kecil dibandingkan dengan AES. 3DES memiliki delay yang lebih kecil dibandingkan dengan AES disebabkan oleh ukuran header dari 3DES yang lebih kecil dibandingkan dengan AES. Hal ini disebabkan karena kecepatan 3DES tidak terpangaruh oleh besarnya ukuran kunci yang digunakan sewaktu proses enkripsi.

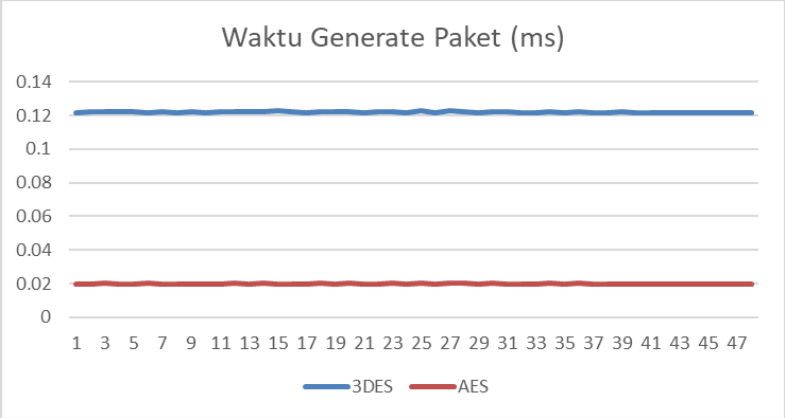
4.1.2 Hasil Pengujian Waktu Pembuatan Paket di MN

Pada pengujian kali ini dilakukan untuk mengukur waktu pembuatan tcp yang telah dienkripsi di MN ke CN.

Tabel 2. Nilai Rata-Rata Waktu generate Paket

Enkripsi	Waktu Generate Paket (ms)
3DES	0.12193
AAES	0.019957

Percobaan Pembuatan Paket ini dilakukan sebanyak 47 kali seperti terlihat pada Gambar 3, dengan menghasilkan waktu rata-rata seperti terlihat pada Tabel 2. Waktu pembuatan paket 3DES memiliki waktu yang lebih lama dibandingkan dengan AES. 3DES memiliki waktu pembuatan paket yang lebih lama dikarenakan dalam proses enkripsi 3DES melakukan 3 proses (enkripsi-dekripsi-enkripsi) menggukanan 3 kunci berbeda.



Gambar 3. Grafik Waktu generate Paket

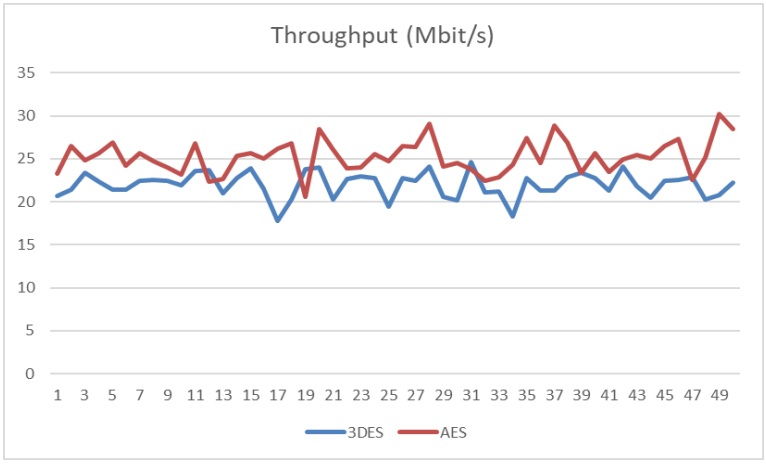
4.1.3 Hasil Pengujian Throughtput MN ke CN

Pengujian kali ini dilakukan untuk mengetahui kecepatan sebenarnya dari MN ketika mengirimkan paket yang telah dienkripsi.

Tabel 3. Nilai Rata-Rata Throughtput

Enkripsi	Throughtput
3DES	21.978 Mbit/s
AES	25.25 Mbit/s

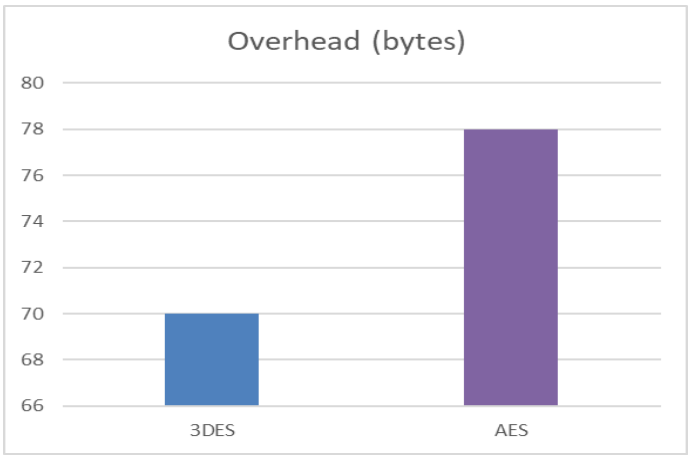
Pengujian *throughput* dari MN ke CN ini dilakukan sebanyak 49 kali dengan hasil seperti terlihat pada Gambar 4. Pada percobaan ini didapatkan hasil dengan 3DES mendapatkan nilai rata-rata sebesar 21.978 Mbit/s dan AES mendapatkan nilai rata-rata 25.25 Mbit/s. Pada pengujian *throughtput* AES masih lebih unggul dibandingkan dengan 3DES.



Gambar 4 Grafik throughtput

4.1.4 Nilai Overhead Paket MN

Pengujian kali ini dilakukan untuk mengetahui besarnya overhead dari paket MN yang telah dienkripsi.



Gambar 5. Grafik Overhead

Overhead merupakan packet header yang digukan algortima enkripsi pada proses enkripsi yang dapat mempengaruhi kecepatan transmisi dari data mentah. Pada Gambar 5 dapat dilihat bahwa AES memiliki ukuran paket overhead yang lebih besar dibandingkan dengan 3DES. Hal ini menyebabkan AES memiliki nilai delay yang lebih besar daripada 3DES seperti terlihat pada Tabel 1.

5. KESIMPULAN

5.1. Kesimpulan

Berdasarkan pengujian dan hasil yang didapatkan, dapat diberikan kesimpulan bahwa, enkripsi digunakan pada MIPv6 untuk mengamankan data yang akan dikirimkan MN ketika melakukan handover

Hasil pengujian delay dan jitter jika menggunakan 3DES mendapatkan hasil rata-rata 27,48 ms dan 39,56 ms sedangkan AES mendapatkan hasil rata-rata 34,68 ms dan 52,73. Nilai dari delay dan jitter dapat dipengaruhi penerimaan sinyal karena percobaan dilakukan dengan keadaan MN bergerak dan berpindah dari HA ke FA.

Hasil pengujian pembentukan paket menujukkan AES memiliki keunggulan daripada 3DES dengan waktu 0,019 ms sedangkan DES memerlukan waktu 0,121 ms. Pada pengujian *throughput* AES juga mengungguli 3DES dengan nilai 25,25 Mbit/s sedangkan 3DES 21,978 Mbit/s.

Berdasarkan pengujian yang sudah dilakukan AES memberikan performansi yang lebih baik daripada 3DES. Meskipun AES memiliki nilai delay dan jitter yang lebih besar dibandingkan dengan

3DES, tetapi AES memiliki kecepatan pembuatan paket dan *throughput* yang lebih baik dibandingkan dengan 3DES.

REFERENSI

[1] Bagus Seta Inba C dan Waskitho Wibisono. *Vertical Handover Berbasis Android Pada Aplikasi Streaming Stored Video*. 2016. Surabaya.

[2] Valdo Marcelino. *Pengukuran Dan Analisis Parameter QOS Pada Jaringan Mobile IPv6 untuk Aplikasi Game Online*. 2012. Depok.

[3] Alhofiki Abdurachman. *Analisis Handover Pada Heterogeneous Network Menggunakan Objek Bergerak Dengan Parameter Handover Trigger*. 2017. Bandar Lampung.

[4] Johnson, D., Perkins, C., and J. Arkko. *Mobility Support in IPv6*. July 2011. RFC 6275. https://tools.ietf.org/html/rfc6275

[5] Aleisa Noura. *A Comparison of the 3DES and AESS encryption standards*. 2016. Scotland.

[6] Hamdan, O., Zaidan, B., Zaidan, A., Hamid, A., Shabbir, M., Al-Nabhani, Y. *New Comparative Study Between DES, 3DES and AES with Nine Factors*. 2010. Kuala Lumpur.

[7] Drestantiarto, Suwega. *Analisa Performa Jaringan Mobile IPv6 Pada Horizontal Handover dan Vertical Handover Dengan Palikasi FTP*. 2012. Depok.